

**IN THE UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

M.S. and D.H., individually and on behalf of
all others similarly situated,

Plaintiffs,

v.

MEDDATA, Inc.,

Defendant.

Case No. 4:22-cv-00187

Hon. Charles Eskridge

PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	SUMMARY OF FACTS DEVELOPED THROUGH DISCOVERY	2
III.	ARGUMENT & AUTHORITIES	4
A.	THE NAMED PLAINTIFFS HAVE STANDING.	4
B.	PLAINTIFFS SATISFY ALL REQUIREMENTS UNDER FEDERAL RULE OF CIVIL PROCEDURE 23.	4
C.	THE PROPOSED CLASSES MEET THE REQUIREMENTS OF RULE 23(A).....	5
1.	<i>Numerosity.</i>	5
2.	<i>Commonality.</i>	6
3.	<i>Typicality.</i>	7
4.	<i>Adequacy.</i>	8
5.	<i>Ascertainability.</i>	9
D.	CERTIFICATION OF THE CLASS UNDER RULE 23(B)(3) IS PROPER.	10
1.	<i>Common Issues of Law and Fact Predominate</i>	10
2.	<i>Class Litigation is Superior to Any Alternative.</i>	19
IV.	CONCLUSION	20

TABLE OF AUTHORITIES

Cases

<i>Almon v. Conduent Bus. Servs., LLC</i> , No. SA-19-CV-01075-XR, 2022 WL 902992 (W.D. Tex. Mar. 25, 2022).....	10
<i>Amgen Inc. v. Connecticut Ret. Plans & Trust Funds</i> , 133 S. Ct. 1184 (2013).....	5, 10
<i>Atl. Marine Constr. Co. v. U.S. Dist. Court for W. Dist. of Tex.</i> , 571 U.S. 49 (2013).....	17
<i>Bell Atlantic Corp. v. AT&T Corp.</i> , 339 F.3d 294 (5th Cir. 2003).....	16
<i>Castano v. Am. Tobacco Co.</i> , 84 F.3d 734 (5th Cir.1996)	19
<i>Cates v. Creamer</i> , 431 F.3d 456 (5th Cir. 2005).....	18
<i>Chakejian v. Equifax Info. Servs. LLC</i> , 256 F.R.D. 492 (E.D. Pa. 2009)	8
<i>Disalvatore v. Foretravel, Inc.</i> , 2016 WL 3951426 (E.D.Tex., 2016).....	19
<i>Eisen v. Carlisle & Jacquelin</i> , 417 U.S. 156 (1974).....	5
<i>Gene & Gene LLC v. BioPay LLC</i> , 541 F.3d 318 (5th Cir. 2008)	4
<i>Glycobiosciences, Inc. v. Woodfield Pharmaceutical, LLC</i> , No. 4:15-CV-02109, LLC, 2016 WL 1702674 (S.D. Tex., 2016).....	19
<i>Grays Harbor Adventist Christian Sch. v. Carrier Corp.</i> , 242 F.R.D. 568 (W.D. Wash. 2007).....	15
<i>Hashemi v. Bosley, Inc.</i> , No. CV-21-946, 2022 WL 2155117 (C.D. Cal. Feb. 22, 2022)	11
<i>Hope v. Nissan N. Am., Inc.</i> , 353 S.W.3d 68 (Mo. Ct. App. 2011).....	15
<i>In re Anthem, Inc. Data Breach Litig.</i> , 327 F.R.D. 299 (N.D. Cal. 2018)	7, 8, 11, 18

<i>In re Brinker Data Incident Litig.</i> , No. 3:18-CV-686-TJC-MCR, 2021 WL 1405508 (M.D. Fla. Apr. 14, 2021)	passim
<i>In re Deepwater Horizon</i> , 739 F.3d 790 (5th Cir. 2014).....	5, 6, 16
<i>In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.</i> , 851 F. Supp. 2d 1040 (S.D. Tex. 2012).....	5, 8, 11
<i>In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.</i> , 341 F.R.D. 128 (D. Md. 2022).....	7, 13
<i>In re McCormick & Co., Inc., Pepper Prod. Mktg. & Sales Pracs. Litig.</i> , 422 F. Supp. 3d 194 (D.D.C. 2019).....	15
<i>In re Premera Blue Cross Customer Data Sec. Breach Litig.</i> , No. 3:15-MD-2633-SI, 2019 WL 3410382 (D. Or. July 29, 2019)	12, 18
<i>In re Target Corp. Customer Data Sec. Breach Litig.</i> , 309 F.R.D. 482 (D. Minn. 2015)	19
<i>In re the Home Depot, Inc., Customer Data Sec. Breach Litig.</i> , No. 1:14-MD-02583- TWT, 2016 WL 6902351 (N.D. Ga. Aug. 23, 2016).....	11
<i>In re Wawa, Inc. Data Sec. Litig.</i> , No. CV-19-6019, 2021 WL 3276148 (E.D. Pa. July 30, 2021).....	11
<i>In re Yahoo Mail Litig.</i> , 308 F.R.D. 577 (N.D. Cal. 2015)	15
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , No. 16-MD-02752-LHK, 2020 WL 4212811 (N.D. Cal. July 22, 2020)	11
<i>Jenkins v. Raymark Indus., Inc.</i> , 782 F.2d 468 (5th Cir. 1986).....	6
<i>John v. Nat’l Sec. Fire & Cas. Co.</i> , 501 F.3d 443 (5th Cir. 2007).....	4

<i>Kostka v. Dickey’s Barbecue Restaurants, Inc.</i> , No. 3:20-CV-03424-K, 2022 WL 16821685 (N.D. Tex. Oct. 14, 2022)	9, 10
<i>Menocal v. GEO Grp. Inc.</i> , 882 F.3d 905 (10th Cir. 2018)	14
<i>Morrow v. Washington</i> , 277 F.R.D. 172 (E.D. Tex. 2011)	9
<i>Mullen v. Treasure Chest Casino, LLC</i> , 186 F.3d 620 (5th Cir. 1999).....	6, 12
<i>Murphy v. Stonewall Kitchen, LLC</i> , 503 S.W.3d 308 (Mo. Ct. App. 2016)	15
<i>Ngethpharat v. State Farm Mut. Ins. Co.</i> , 339 F.R.D. 154 (W.D. Wash. 2021).....	14
<i>Reichert v. Keefe Commissary Network, L.L.C.</i> , 331 F.R.D. 541 (W.D. Wash. 2019).....	15
<i>Rivera v. S. Green Ltd. P’ship</i> , 208 S.W.3d 12 (Tex. App. 2006)	13
<i>Romero v. Securus Techs., Inc.</i> , 331 F.R.D. 391 (S.D. Cal. 2018)	13
<i>Ruiz Torres v. Mercer Canyons Inc.</i> , 835 F.3d 1125 (9th Cir. 2016)	14
<i>Smith v. Triad of Ala., LLC</i> , No. 1:14-cv-324-WKW, 2017 WL 1044692 (M.D. Ala. Mar. 17, 2017).....	12, 13
<i>Spence v. Glock, Ges.m.b.H.</i> , 227 F.3d 308 (5th Cir. 2000)	17
<i>Tyson Foods, Inc. v. Bouaphakeo</i> , 577 U.S. 442 (2016)	10, 16
<i>Unger v. Amedisys Inc.</i> , 401 F.3d 316 (5th Cir. 2005).....	9
<i>Valenzuela v. Aquino</i> , 853 S.W.2d 512 (Tex. 1993)	13
<i>Vine v. PLS Fin. Servs., Inc.</i> , 331 F.R.D. 325 (E.D. Tex. 2019)	7
<i>Welsh v. Navy Fed. Credit Union</i> , No. 5:16-CV-1062-DAE, 2018 WL 7283639 (W.D. Tex. Aug. 20, 2018)	4, 5, 6, 8

Statutes

Federal Rule of Civil Procedure 23passim

I. INTRODUCTION

Plaintiffs M.S. and Plaintiff D.H. (collectively, “Plaintiffs”) brought this action as a result of their protected health information (“PHI”) and personal identifiable information (“PII”) being unlawfully posted by Defendant MedData, Inc. (“Defendant” or “MedData”) to a public-facing website for over thirteen (13) months, along with the PHI and PII of approximately 140,000 other individuals. The files were accessed thousands of times and “cloned” multiple times by unknown individuals. As a result of Defendant’s actions, the Class’s PHI and PII is in the hands of unauthorized persons who already have and will continue to use the PHI to commit identity theft and other crimes.

Plaintiffs move, pursuant to Fed. R. Civ. P. 23(a) and (b)(3), for an Order to certify the following Nationwide Class and Missouri Subclass (collectively, the “Class”):

Nationwide Class

All persons residing in the United States and its Territories whose PII or PHI was exposed as a result of the MedData Healthcare Data Breach that occurred from sometime between December 2018 and September 2019 through December 17, 2020.

Missouri Subclass

All persons residing in Missouri whose PII and PHI was exposed as a result of the MedData Healthcare Data Breach that occurred from sometime between December 2018 and September 2019 through December 17, 2020.

Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

Plaintiffs further move the Court for an order appointing Plaintiffs as Class Representatives and Federman & Sherwood and McShane & Brady LLC as Class Counsel.

II. SUMMARY OF FACTS

MedData is a company that provides healthcare revenue cycle management services to healthcare facilities nationwide. In order to provide these services, MedData takes possession of its clients' patients' PHI and PII.

In November 2020, MedData was notified by security researcher Jelle Ursem that some of its clients' patients' PII and PHI was discovered on the public software development website Github. Declaration of Jelle Ursem ¶ 3, ECF No. 58-1 After repeated messages from Ursem, MedData finally launched an investigation. *Id.* ¶ 11. The investigation revealed at least one of MedData's employees saved files containing patients' PHI and PII to GitHub between December 2018 and September 2019. Declaration of Zulfiqar Faruqi ¶¶ 4–6, ECF No. 67-1. The exposed PHI and PII included: (1) patient contact information (such as patient names, addresses, and dates of birth); (2) Social Security numbers; (3) diagnoses; (4) medical conditions; (5) claims information; (6) dates of service; (7) subscriber IDs; (8) medical procedure codes; (9) provider names; and (10) health insurance policy numbers. *See* Compl. ¶ 7, ECF No. 1; *see also* Exhibit 1, 30(b)(6) Deposition, at 26:2–20. These files were eventually removed by Defendant ***thirteen months*** after they were uploaded. Exhibit 1, 30(b)(6) Dep., at 33:23–34:12; 173:12–24; 176:6–21. However, the damage was done – unknown individuals had accessed the PHI and PII, and it was “cloned” thirty-five times. *Id.* at 40:10–42:3; *see also* MD6735 (ECF No. 58-2). Despite knowing of the breach for months, MedData did not notify Plaintiffs

and Class Members that their data was exposed until March 31, 2021. Exhibit 1, 30(b)(6) Dep., at 161:21–162:25.

This Data Breach was preventable.

114

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

5

MedData senior software developer Bobby Faruqi had access to sensitive and confidential PHI and PII, failed to keep the sensitive data secure, and posted the patient PHI and PII to a public website. Faruqi Decl. (ECF No. 67-1), ¶¶ 2-6. MedData's General Counsel acknowledged that developers

like Mr. Faruqi “had regular access to PHI” and that while “PHI is stored on secure shared drives ... it is common for developers to download that data to their computers when doing working/testing etc.” Exhibit 3 (MD6724-25) at MD6725. Only after the Data Breach did MedData take steps to restrict employees from exporting data to sites like GitHub. *See* Exhibit 1 (30(b)(6) Dep.) at 96:18-98:5, 119:21-120:12.

III. ARGUMENT & AUTHORITIES

A. Plaintiffs Have Standing

Plaintiffs established their Article III standing in their response to MedData’s motion to dismiss by demonstrating injury-in-fact in the actual data misuse they have already experienced, the increased risk of harm they face, the time, effort, and money spent to mitigate the effects of the increased risk of harm, and that they lost the value of their private, personal information. ECF No. 58.

B. Plaintiffs Satisfy All Requirements Under Federal Rule of Civil Procedure 23

Rule 23(a) lists four initial criteria plaintiffs must meet for class certification – numerosity, commonality, typicality, and adequacy. *Gene & Gene LLC v. BioPay LLC*, 541 F.3d 318, 325 (5th Cir. 2008); *Welsh v. Navy Fed. Credit Union*, No. 5:16-CV-1062-DAE, 2018 WL 7283639, at *7 (W.D. Tex. Aug. 20, 2018). The Fifth Circuit has also interpreted Rule 23(a) to contain an implied prerequisite of ascertainability. *See John v. Nat’l Sec. Fire & Cas. Co.*, 501 F.3d 443, 445 n.3 (5th Cir. 2007).

The final step in class certification is satisfying one of the class types defined in Rule 23(b). Certification under Rule 23(b)(3) requires the Court find “(1) common issues

of law or fact *predominate* over any questions affecting only individual members; and (2) a class action is *superior* to other available methods for fairly and efficiently adjudicating the controversy.” *Welsh*, 2018 WL 7283639 at *7 (emphasis added).

In determining whether class certification is appropriate, “the question is not whether the plaintiff or plaintiffs have stated a cause of action or will prevail on the merits, but rather whether the requirements of Rule 23 are met.” *Eisen v. Carlisle & Jacquelin*, 417 U.S. 156, 177–78 (1974). “Rule 23 grants courts no license to engage in free-ranging merits inquiries at the certification stage.” *Amgen Inc. v. Connecticut Ret. Plans & Trust Funds*, 133 S. Ct. 1184, 1194–95 (2013). The class certification stage is not a “dress rehearsal on the merits.” *In re Deepwater Horizon*, 739 F.3d 790, 811 (5th Cir. 2014). Instead, Plaintiffs need only “establish[] the Rule 23 requirements by a preponderance of the evidence.” *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 851 F. Supp. 2d 1040, 1052 (S.D. Tex. 2012).

As discussed below, this case easily satisfies Rule 23’s prerequisites.

C. The Proposed Classes Meet the Requirements of Rule 23(a)

1. Numerosity

Rule 23(a)(1) requires the class be “so numerous that joinder of all members is impracticable.” Fed. R. Civ. P. 23(a)(1). Plaintiffs clearly satisfy this requirement because approximately 140,000 patients’ PII and PHI was exposed in the Data Breach, and

attempting to join all victims would be near impossible.¹ *See* Exhibit 4 (MedData’s Response to Interrogatory No. 21) at 15–16. As such, numerosity is met. *See Mullen v. Treasure Chest Casino, LLC*, 186 F.3d 620, 624 (5th Cir. 1999) (noting that 100 to 150 members “is within the range that generally satisfies the numerosity requirement”); *Welsh*, 2018 WL 7283639 at *5 (numerosity satisfied where the proposed class contained approximately two thousand members).

2. Commonality

Rule 23(a)(2) requires “questions of law or fact common to the class.” The threshold of commonality is not high. *Jenkins v. Raymark Indus., Inc.*, 782 F.2d 468, 472 (5th Cir. 1986). This requirement can be satisfied “by an instance of defendant’s injurious conduct even when the resulting injurious effects – the damages – are diverse.” *See In re Deepwater Horizon*, 739 F.3d at 810–11.

Here, commonality is satisfied because there are significant questions of fact and law that are common to Class Members. These questions include: (1) whether MedData had a duty to protect Class Members’ PHI and PII; (2) whether MedData’s security measures were inadequate; (3) whether MedData knew or should have known that Class Members’ PHI and PII was vulnerable to exposure; and (4) whether MedData timely notified Class Members that their PHI and PII was disclosed.

¹ *See* <https://apps.web.maine.gov/online/aevviewer/ME/40/1a0b61cf-1aab-44ad-b839-feb6d76af693.shtml> (identifying 135,908 affected individuals).

As courts have found in similar cases, these common questions will generate common answers that will drive resolution of this litigation. *See In re Brinker Data Incident Litig.*, No. 3:18-CV-686-TJC-MCR, 2021 WL 1405508, at *8 (M.D. Fla. Apr. 14, 2021) (finding commonality satisfied by questions of “whether Brinker had a duty to protect customer data, whether Brinker knew or should have known its data systems were susceptible, and whether Brinker failed to implement adequate data security measures to protect customers’ data”); *see also In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 341 F.R.D. 128, 147 (D. Md. 2022) (“Common questions of fact include whether Defendants knew about their data security vulnerabilities, what Defendants did or did not do to address those vulnerabilities, and whether the hacker(s) exploited those vulnerabilities to exfiltrate customers’ PII.”); *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 308 (N.D. Cal. 2018) (The extensiveness and adequacy of Anthem’s security measures lie at the heart of every claim. ... Related factual questions about whether Anthem knew that its data security was inadequate and whether Anthem amply responded to the data breach also apply uniformly across the entire Class.”).

3. Typicality

Typicality is satisfied if “the claims or defenses of the representative parties are typical of the claims or defenses of the class.” Fed. R. Civ. P. 23(a)(3). “Like commonality, the test for typicality is not demanding.” *Vine v. PLS Fin. Servs., Inc.*, 331 F.R.D. 325, 333 (E.D. Tex. 2019), *aff’d*, 807 F. App’x 320 (5th Cir. 2020). “[T]he critical inquiry is whether

the class representative's claims have the same essential characteristics of those of the putative class." *In re Heartland Payment Sys., Inc.*, 851 F. Supp. 2d at 1054.

Here, Plaintiffs and the Class were injured through Defendant's Data Breach. Thus, Plaintiffs' claims and legal theories, both in their individual and representative capacities, arise under the same factual predicate. Further, there are no defenses unique to Plaintiffs. Therefore, Plaintiffs satisfy typicality. *See id.* ("If the claims arise from a similar course of conduct and share the same legal theory, factual differences will not defeat typicality."); *see also Brinker*, 2021 WL 1405508 at *8 (finding typicality satisfied where plaintiffs' and Class Members' injuries arose out of the same data breach and they asserted the same claims); *Anthem*, 327 F.R.D. at 309 (typicality satisfied where "the lawsuit ha[d] a narrow focus—namely, to challenge the sufficiency of [the defendant's] data security and receive adequate compensatory damages for the breach of [the defendant's] system"); *Welsh*, 2018 WL 7283639 at *6 (finding the plaintiff's claims were typical because the plaintiff's claims arose out of the same conduct); *Chakejian v. Equifax Info. Servs. LLC*, 256 F.R.D. 492, 498 (E.D. Pa. 2009) (typicality satisfied where "[t]he claims of [the class representative] and each of the prospective Class Members arise from the same course of conduct, and are based on the same theory of liability").

4. Adequacy

To meet the adequacy requirement, "the court must find that [the] class representatives, their counsel, and the relationship between the two are adequate to protect the interests of absent Class Members." *Unger v. Amedisys Inc.*, 401 F.3d 316, 321 (5th

Cir. 2005). This requirement is satisfied when proposed class counsel is qualified and competent to prosecute the action, and the interests of the proposed class representatives do not conflict with the interests of the class. *See Morrow v. Washington*, 277 F.R.D. 172, 195 (E.D. Tex. 2011); *Kostka v. Dickey's Barbecue Restaurants, Inc.*, No. 3:20-CV-03424-K, 2022 WL 16821685, at *7 (N.D. Tex. Oct. 14, 2022).

Plaintiffs have no antagonistic or conflicting interest with the members of the proposed class. To the contrary, Plaintiffs have demonstrated their commitment to the class by actively participating in the litigation. Plaintiffs have worked with counsel to develop the class claims, respond to discovery, and prepare for depositions. Plaintiffs have also retained experienced and capable counsel who will vigorously prosecute the class claims. *See* Exhibit 5, Federman & Sherwood Firm Resume; *see also* Exhibit 6, McShane & Brady, LLC Firm Resume. Plaintiff's counsel have devoted a significant time to investigating the potential claims and will continue to commit time and resources necessary to represent the class. Plaintiff's counsel also have substantial experience in litigating class action lawsuits addressing data breaches and privacy issues, and have been appointed to serve as class counsel in similar cases. *Id.* Plaintiffs and their counsel have demonstrated their commitment to prosecuting this case on behalf of all Class Members and therefore satisfy the adequacy requirement.

5. Ascertainability

“[T]he touchstone of ascertainability is whether the class is sufficiently definite so that it is administratively feasible for the court to determine whether a particular individual

is a member.” *Kostka Inc.*, 2022 WL 16821685 at *8 (citation omitted)). Ascertainability is met when the class is “identifiable by objective criteria.” *Almon v. Conduent Bus. Servs., LLC*, No. SA-19-CV-01075-XR, 2022 WL 902992, at *24 (W.D. Tex. Mar. 25, 2022).

Here, the proposed Class meets the ascertainability requirement because Defendant can readily determine from its own records who is a Class Member. Defendant sent Notice letters to persons impacted by the Data Breach; thus, Defendant has already determined who is a Class Member. This objective criterion is sufficient for ascertainability purposes. *Id.* (“[T]he Court is satisfied that the proposed classes are ascertainable from the records maintained in Defendants’ ordinary course of business.”).

D. Certification of the Class Under Rule 23(b)(3) is Proper

1. Common Issues of Law and Fact Predominate

Predominance is satisfied when “the common, aggregation-enabling, issues in the case are more prevalent or important than the non-common, aggregation-defeating, individual issues.” *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016) (citation omitted). “An individual question is one where members of a proposed class will need to present evidence that varies from member to member, while a common question is one ... susceptible to generalized, class-wide proof.” *Id.* However, Plaintiffs do not need to “prove that *each* ‘element of [their] claim[s] [are] susceptible to classwide proof.’” *Amgen*, 568 U.S. at 469 (citation and alterations omitted).

i. Common Questions Present a Significant Aspect of the Case

All class members' claims stem from a single event: the exposure of their data by MedData's employee on the GitHub website. Plaintiff's claims focus on whether MedData used reasonable security measures to protect class members' PHI and PII. Courts routinely recognize that claims arising from unauthorized disclosures of PHI and PII turn on common questions that are proven with predominantly common evidence. *See, e.g., In re Heartland Payment Sys., Inc.*, 851 F. Supp. 2d at 1059; *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2020 WL 4212811, at *7 (N.D. Cal. July 22, 2020), *aff'd*, No. 20-16633, 2022 WL 2304236 (9th Cir. June 27, 2022); *See Hashemi v. Bosley, Inc.*, No. CV-21-946, 2022 WL 2155117, at *4 (C.D. Cal. Feb. 22, 2022); *In re Wawa, Inc. Data Sec. Litig.*, No. CV-19-6019, 2021 WL 3276148, at *4 (E.D. Pa. July 30, 2021); *Anthem*, 327 F.R.D. at 312; *In re the Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-02583-TWT, 2016 WL 6902351, at *2 (N.D. Ga. Aug. 23, 2016).

a. Negligence and Breach of Fiduciary Duty Claims

In a case such as this, where the operative conduct giving rise to both the duty and breach is uniform, Plaintiffs' negligence claim is appropriate for class wide resolution. *Brinker*, 2021 WL 1405508 at *11. Each Class Member gave their PHI and PII to Defendant, each alleges their PHI/PII was unlawfully exposed and accessed from the same GitHub posting, and each suffered the same general type of damages. Thus, questions of duty, Defendant's breach, and damages are common issues susceptible to common proof. *See, e.g., Smith v. Triad of Ala., LLC*, No. 1:14-cv-324-WKW, 2017 WL 1044692, at *13

(M.D. Ala. Mar. 17, 2017). Indeed, these legal questions will be resolved by common evidence, including MedData’s policies and procedures, testimony of MedData employees, and expert testimony. Numerous courts have certified classes where, as is here, the negligent act and resulting damages form a common set of operative facts. *See, e.g., Mullen*, 186 F.3d at 626; *Brinker*, 2021 WL 1405508, at *8, 11 (certifying nationwide class and finding common questions predominate the negligent claim: “whether Brinker had a duty to protect customer data, whether Brinker knew or should have known its data systems were susceptible, and whether Brinker failed to implement adequate data security measures to protect customers’ data”); *In re Premiera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2019 WL 3410382, at *18 (D. Or. July 29, 2019) (“Premera’s duty, if any, to protect Sensitive Information, would be owed classwide and whether that duty was breached also would be a class question.... Plaintiffs also had two theories of damages that involved class-wide proof and apply uniformly.”).

Plaintiffs’ breach of fiduciary duty claim succeeds for the same reasons Plaintiffs’ negligence claims succeed. The existence of the fiduciary duty and whether Defendant breached this duty does not differ between Class Members. These claims are grounded in Defendant’s conduct towards the entire class. The same actions (inadequate security measures) by a single actor (Defendant) caused the same injury to all Class Members (compromise of their PHI and PII).

b. Contract-Based Claims

Both the existence of the implied contract and its breach are factors to be determined on a class-wide basis. The implied contract is one between Defendant and all individuals whose PII/PHI is maintained by Defendant, and company-level failures that led to the breach. These facts will not vary among Class Members. *See Smith*, 2017 WL 1044692, at *12 (finding implied-contract claim “passes the predominance criterion” in data breach case); *In re Marriott Int’l, Inc.*, 341 F.R.D. at 157 (same).

Whether MedData breached third-party beneficiary contracts is also determined through common proof. To recover, plaintiffs must show: “(1) the contracting parties intended to benefit the third-party beneficiary; and (2) the parties entered into the contract direct and primarily for the third party’s benefit.” *Rivera v. S. Green Ltd. P’ship*, 208 S.W.3d 12, 22 (Tex. App. 2006). Defendant entered into contracts with medical facilities, primarily for the benefit of Class Members. Whether these contracts were breached turns on common facts, which again, spawn from Defendant’s conduct.

c. Invasion of Privacy

Plaintiffs’ invasion of privacy claim turns on MedData’s conduct and whether the intrusion is highly offensive to a reasonable person based on an objective standard. *See Valenzuela v. Aquino*, 853 S.W.2d 512, 513 (Tex. 1993) (providing elements of invasion of privacy). Neither element requires individual Class Member evidence. *Cf. Romero v. Securus Techs., Inc.*, 331 F.R.D. 391, 410 (S.D. Cal. 2018) (finding predominance for California’s Invasion of Privacy Act).

d. Unjust Enrichment

Here, Plaintiffs allege MedData was unjustly enriched by obtaining monetary benefits for the secure processing of patients’ medical billings and claims, without having implemented the reasonable and legally mandated data security measures. The facts and law supporting the improper retention of these proceeds are the same without regard to individualized circumstances. Indeed, Plaintiffs’ unjust enrichment claim merits class certification. *See Menocal v. GEO Grp. Inc.*, 882 F.3d 905, 923–27 (10th Cir. 2018) (explaining that Rule 23(b)(3)’s predominance requirement does not prohibit class certification of unjust enrichment claims).

e. Washington Consumer Protection Act (“WCPA”)

Plaintiffs’ WCPA claim is proven with class-wide proof. A WCPA claim requires five elements: “(1) an unfair or deceptive act or practice; (2) which occurs in trade or commerce; (3) that impacts the public interest; (4) which causes injury to the plaintiff in his or her business or property; and (5) which injury is causally linked to the unfair or deceptive act.” *Ruiz Torres v. Mercer Canyons Inc.*, 835 F.3d 1125, 1135 (9th Cir. 2016).

Each Plaintiff alleges Defendant failed to safeguard their PHI and PII, in the conduct of its business, which has resulted in the public disclosure of Plaintiffs’ and the Class’s PHI and PII. Due to the Data Breach, Plaintiffs suffered common injuries – out-of-pocket mitigation costs, diminution in value of their PII and PHI, and lost time. Furthermore, Courts routinely certify WCPA claims on a class wide basis. *Id.*; *Ngethpharat v. State Farm Mut. Ins. Co.*, 339 F.R.D. 154, 167 (W.D. Wash. 2021); *Reichert v. Keefe Commissary*

Network, L.L.C., 331 F.R.D. 541, 556 (W.D. Wash. 2019) (“injury and causation, [] do not defeat predominance”); *Grays Harbor Adventist Christian Sch. v. Carrier Corp.*, 242 F.R.D. 568, 574 (W.D. Wash. 2007).

f. Missouri Merchandising Practices Act (“MMPA”)

Similarly, Plaintiffs’ MMPA claim will be based on common evidence. Whether Defendant’s inadequate data security measures and the resulting Data Breach constitute an “unlawful act” under the MMPA is an issue common to all Class Members. *See Murphy v. Stonewall Kitchen, LLC*, 503 S.W.3d 308, 311 (Mo. Ct. App. 2016) (setting forth MMPA elements). Similarly, the elements of causation and ascertainable loss are common to all Class Members. As a direct result of Defendant’s unlawful act, Defendant caused an ascertainable loss to Class Members who did not receive the privacy protections entitled to them. Thus, Plaintiffs’ MMPA claim will rise or fall on a class-wide basis, and common questions predominate. *See In re McCormick & Co., Inc., Pepper Prod. Mktg. & Sales Pracs. Litig.*, 422 F. Supp. 3d 194, 263 (D.D.C. 2019); *See also Hope v. Nissan N. Am., Inc.*, 353 S.W.3d 68, 84 (Mo. Ct. App. 2011).

g. Declaratory and Injunctive Relief

Lastly, Plaintiffs’ claim for declaratory and injunctive relief is certifiable. Under Rule 23(b)(2), it is “sufficient if class members complain of a pattern or practice that is generally applicable to the class as a whole.” *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 598 (N.D. Cal. 2015) (citation omitted). “Unlike Rule 23(b)(3), a plaintiff does not need to

show predominance of common issues or superiority of class adjudication to certify a Rule 23(b)(2) class.” *Id.* at 587.

Defendant’s inadequate security protocols and procedures resulted in the compromise of the PII/PHI of all Class Members, causing each Class Member to suffer loss of value in their PII and/or PHI and to incur out-of-pocket mitigation costs. It is also believed that Defendant still possesses and inadequately protects all Class Members PII and PHI. Therefore, no individualized proof is needed for this claim.

ii. Damages Will Be Determined Using a Class-wide Methodology

“When one or more of the central issues in the action are common to the class” and “predominate,” a class is certifiable even where members have individualized damages. *Tyson Foods*, 577 U.S. at 453; *see Bell Atlantic Corp. v. AT&T Corp.*, 339 F.3d 294, 306 (5th Cir. 2003) (“Even wide disparity among class members as to the amount of damages” does not preclude class certification ”and courts, therefore, have certified classes even in light of the need for individualized calculations of damages.”). As demonstrated above, Plaintiffs’ claims present several common questions. Thus, even if the determination of class members’ damages ultimately requires individual calculations or proof, the common liability issues warrant certification. *In re Deepwater Horizon*, 739 F.3d at 815 (holding that *Comcast* “has no impact on cases such as the present one, in which predominance was based not on common issues of damages but on the numerous common issues of liability”).

Nonetheless, Plaintiffs intend to proffer expert testimony to help quantify damages. Plaintiffs’ expert, Gary Olsen, explains that damages can be calculated on a class-wide

basis in this case using a damages methodology that is directly tied to Plaintiffs' theories of liability. Mr. Olsen has grouped Class Members into four categories based on the type of information disclosed and provided three methods for calculating Class Members' damages based on these categories. Exhibit 7 (Expert Report) ¶¶ 5-11, 16, 27-28; [REDACTED]

[REDACTED]. Mr. Olsen further demonstrates how these methods can be applied to arrive at class-wide damages for: (1) the unauthorized access of Class Members' PII/PHI; (2) the increased risk of identity theft; and (3) "benefit of the bargain" damages. *Id.* 29-66. Thus, while not required, Plaintiffs will be able to prove damages for all Class Members using common evidence and common damages formulae, further demonstrating that common issues predominate throughout the case.

iii. *Choice-of-Law Analysis Confirms Common Questions Predominate*

Because Plaintiffs seek to certify a nationwide class of all persons whose data was exposed, choice-of-law issues could impact predominance. Here, however, the outcome of the choice-of-law inquiry confirms it is no barrier to class certification and Texas law applies.

A "federal court sitting in diversity ordinarily must follow the choice-of-law rules of the State in which it sits." *Atl. Marine Constr. Co. v. U.S. Dist. Court for W. Dist. of Tex.*, 571 U.S. 49, 65 (2013). As the forum state, Texas uses the "most significant relationship test." *Spence v. Glock, Ges.m.b.H.*, 227 F.3d 308, 311 (5th Cir. 2000) (internal citation omitted). The first step is to determine if there is an actual conflict. *See Cates v.*

Creamer, 431 F.3d 456, 464 (5th Cir. 2005). If an actual conflict is identified, the governing law is determined by considering the following factors: (1) the place where the injury occurred; (2) the place where the conduct causing the injury occurred; (3) the domicile, residence, nationality, place of incorporation and place of business of the parties; and (4) the place where the relationship, if any, between the parties is centered. *Id.*

First, there is no material conflict among the states' laws. Courts have recognized that the contract and negligence elements are the same in all states and that in data breach cases "the main issue boils down to the common factual contention of whether [defendant]'s data security levels were reasonable" and "the same actions by the same actor wrought the same injury on all ... [c]lass [m]embers together." *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. at 314; *see also In re Premera*, 2019 WL 3410382, at *18 n.6 (certifying nationwide negligence and contract claims in data breach case and noting that there are no meaningful differences in negligence laws in this context).

Second, even if the Court finds substantive conflicts, Texas law still applies. Defendant is headquartered in Texas, the PHI and PII of Plaintiffs and the Class was uploaded by Defendant's employee from Texas, the decisions regarding what steps to take or not take in response to the Data Breach were made in Texas, and the policies and procedures governing Defendant's data security originate from Texas. *See Exhibit 9* (MedData's Motion Re Forum Non Conveniens) at 2-3. Thus, Texas is where the injury (posting of unencrypted PII and PHI onto GitHub) occurred, the conduct causing the injury (Mednax's inadequate data security measures) occurred, MedData is domiciled, and where

the relationship and claims are centered. *See* Exhibit 9 at 6 (“[T]he data security incident that is the basis for each of Plaintiffs’ claims occurred in the Southern District of Texas.”); *see also In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482, 486 (D. Minn. 2015) (location of corporation’s headquarters, computer servers, and where decision regarding the data breach were made were most significant contacts); *Disalvatore v. Foretravel, Inc.*, 2016 WL 3951426 (E.D. Tex., 2016) (applying Texas law where defective RV was purchased in Texas, relevant paperwork was prepared in Texas, and defective RV came from Texas); *Glycobiosciences, Inc. v. Woodfield Pharmaceutical, LLC*, No. 4:15-CV-02109, LLC, 2016 WL 1702674 (S.D. Tex. 2016) (applying Texas law where “the record shows that Texas has a substantial relationship with the parties and the transaction and no other state has a materially greater interest”). Texas, therefore, has the most significant relationship to the claims.

2. Class Litigation is Superior to Any Alternative

A “class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b)(3). Indeed, this is the kind of case for which the class action procedure was created.

First, any Class member’s individual recovery would be dwarfed by the cost of proving the issues in this litigation. The most compelling rationale for finding superiority in a class action” is “the existence of a negative value suit[.]” *Castano v. Am. Tobacco Co.*, 84 F.3d 734, 748 (5th Cir.1996); *see Brinker*, 2021 WL 1405508, at *13 (certifying data breach class and emphasizing that class-wide litigation “will allow for the sharing of

resources and rendering of uniform decisions that cannot be achieved through individual trials”). Second, although two related cases are currently pending against MedData, counsel for the plaintiffs in these cases are working cooperatively. Third, this Court is well positioned to oversee the continued litigation of these claims on a class-wide basis. *See* Exhibit 9 at 2-3 and 6-7. Fourth, the case will be manageable because the central issues are common to all Class Members and will be proven with predominantly common evidence.

IV. CONCLUSION

Because the Rule 23 requirements are satisfied, Plaintiffs respectfully request that the Court certify the proposed Class, appoint Plaintiffs as Class Representatives, and appoint Federman & Sherwood and McShane and Brady LLC as Class Counsel.

Dated: February 23, 2023

Respectfully submitted,

/s/ William B. Federman

William B Federman (TX Bar No. 00794935)

A. Brooke Murphy (admitted *pro hac vice*)

FEDERMAN & SHERWOOD

212 W. Spring Valley Road,
Richardson, Texas 75081

-and-

10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120

Phone: (405) 235-1560

wbf@federmanlaw.com

abm@federmanlaw.com

Maureen M. Brady (admitted *pro hac vice*)

MCSHANE & BRADY LLC

1656 WASHINGTON ST STE 120

KANSAS CITY, MO 64108

816-888-8010

mbrady@mcshanebradylaw.com

Counsel for Plaintiffs

CERTIFICATE OF WORD COUNT

I hereby certify that this document complies with Rule 18 of this Court's Procedures, being 4,979 words (under the Court's limit of 5,000 words), exclusive of case caption, tables, signatures, and certificates.

/s/ William B. Federman
William B. Federman

CERTIFICATE OF CONFERENCE

Pursuant to Local Civil Rule 7.1(D), the parties conferred in good faith on February 14, 2023, however, Counsel could not agree on the disposition of the motion.

/s/ William B. Federman
William B. Federman

CERTIFICATE OF SERVICE

I hereby certify that on February 23, 2023, I caused the foregoing to be electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of the filing to all counsel of record.

/s/ William B. Federman
William B. Federman